JOURNAL OF NUMBER THEORY 5, 433–434 (1973)

A Reconsideration of Legendre–Jacobi Symbols

DENNIS R. ESTES

Department of Mathematics, University of Southern California, Los Angeles, California 90007

AND

GORDON PALL

Department of Mathematics, Louisiana State University, Baton Rouge, Louisiana 70803

PRESENTED AT THE QUADRATIC FORMS CONFERENCE, BATON ROUGE, LOUISIANA, MARCH 27–30, 1972, AND DEDICATED TO THE MEMORY OF LOUIS JOEL MORDELL

The classical definition of the Jacobi symbol $(a:b)$ was badly conceived for negative values of b. Alternative useful definitions of $(a:-1)$ are proposed here. This is an elaboration of a point in the article "Spinor genera of binary quadratic forms" in this issue.

The Legendre–Jacobi symbol was so defined that *if* the congruence $x^2 \equiv a \pmod{b}$ is solvable, and b is prime to $2a$, then $(a : b) = 1$. This is unnecessarily restrictive when b is negative: it would have sufficed for applications to be able to conclude from $x^2 \equiv a \pmod{b}$ that $(a : |b|) = 1$. It seems better to allow the definition of $(a : u)$ when u is a unit to be available to serve other purposes.

In fact, the convention that when b is positive and prime to $2a$,

$$(a : -b) = (a : b), \tag{1}$$

was never entirely satisfactory even for the one use that the symbol should have fitted perfectly: that of expressing generic characters of quadratic forms. For we cannot even properly say that the form f has the generic character $(-1 : f)$ when f represents only one odd residue mod 4, if we insist on having $(-1 : -b) = (-1 : b)$. As a result, mathematicians have long struggled with

$$(-1)^{(f-1)/2} \quad \text{and} \quad (-1)^{(f-1)/2+(f^2-1)/8},$$

when, with another definition for $(a : -1)$, $(f : -1)$ and $(f : -2)$ would have served perfectly.

Some improvement results if we define for b positive and prime to $2a$,

$$\begin{aligned} (a: -b) &= (a : b) \qquad \text{when} \quad a > 0, \\ &= -(a : b) \qquad \text{when} \quad a < 0. \end{aligned} \tag{2}$$

From this follows $(-1 : b) = (-1)^{\frac{1}{2}(b-1)}$ for odd b; and as also from (1),

$$(a : bc) = (a : b)(a : c) \qquad \text{if} \quad (bc, 2a) = 1. \tag{3}$$

From either (1) or (2) follows for odd coprime a, b that

$$(a : b)(b : a) = e \cdot (-1)^{\frac{1}{2}(a-1)\frac{1}{2}(b-1)}, \tag{4}$$

where $e = 1$, except that $e = -1$ when both a and b are negative. However, $(b : -1)$ need not equal $(-1 : b)$.

For the purposes of [1], and perhaps generally, the most satisfactory result appears if we define for b positive and prime to $2a$,

$$\begin{aligned} (a: -b) &= (a : b) \qquad \text{when} \quad a \equiv 1 \bmod 4, \\ &= -(a : b) \qquad \text{when} \quad a \equiv 3 \bmod 4. \end{aligned} \tag{5}$$

Then (3) follows, and also

$$(a : -1) = (-1)^{\frac{1}{2}(a-1)} = (-1 : a) \qquad (a \text{ odd}), \tag{6}$$

and (4) holds with $e = 1$, except that $e = -1$ when both a and b are negative and $a \equiv b \bmod 4$, or only one is negative and the other $\equiv 3 \bmod 4$. Further, with

$$(m : 2) = (2 : m) = (-1)^{(m^2-1)/8} (m \text{ odd}), \tag{7}$$

the symbol $(a : b)$ extends multiplicatively on either component to be defined whenever $(a, b) = 1$; and we have the useful definitions of$(f : p_i)$ in [1] for $p_i = -1$, 2, or -2, and corresponding expressions for spinor-generic characters. It may well be that the theory of genera over the integers, or even over rings, for forms in any number of variables will be substantially advanced if we allow symbols relating to units to be defined in their own right.

Reference

1. Dennis R. Estes and G. Pall, Spinor genera of binary quadratic forms, *J. Number Theory* **5** (1973), 421–432.